Enacting Expertise: Ritual and Risk in Cybersecurity

Shires, James

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Shires, J. (2018). Enacting Expertise: Ritual and Risk in Cybersecurity. *Politics and Governance*, *6*(2), 31-40. https://doi.org/10.17645/pag.v6i2.1329

COGITATIO

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 31–40
DOI: 10.17645/pag.v6i2.1329

Article

Enacting Expertise: Ritual and Risk in Cybersecurity

James Shires

Department of Politics and International Relations, University of Oxford, Oxford, OX1 3UQ, UK;
E-Mail: james.shires@politics.ox.ac.uk

Submitted: 29 December 2017 | Accepted: 12 February 2018 | Published: 11 June 2018

Abstract
This article applies the concept of ritual to cybersecurity expertise, beginning with the cybersecurity "skills gap": the perceived lack of suitably qualified professionals necessary to tackle contemporary cybersecurity challenges. It proposes that cybersecurity expertise is best understood as a skilled performance which satisfies decision-makers' demands for risk management. This alternative understanding of cybersecurity expertise enables investigation of the types of performance involved in key events which congregate experts together: cybersecurity conferences. The article makes two key claims, which are empirically based on participant observation of cybersecurity conferences in the Middle East. First, that cybersecurity conferences are ritualized activities which create an expert community across international boundaries despite significant political and social differences. Second, that the ritualized physical separation between disinterested knowledge-sharing and commercial advertisement at these conferences enacts an ideal of "pure" cybersecurity expertise rarely encountered elsewhere, without which the claims to knowledge made by cybersecurity experts would be greatly undermined. The approach taken in this article is thus a new direction for cybersecurity research, with significant implications for other areas of international politics.

Keywords
conference; cybersecurity; expertise; Middle East; performance; skills gap

Issue
This article is part of the issue "Global Cybersecurity: New Directions in Theory and Methods", edited by Tim Stevens (King's College London, UK).

1. Introduction

In 1944, the team programming the IBM Mark I, a mammoth computing machine built in the US during WWII to assist military calculations, had a surprising routine:

> When the program was punched into a tape and the moment came to test it, the Mark I crew, as a joke that became a ritual, would pull out a prayer rug, face east, and pray that their work would prove acceptable. (Isaacson, 2015)

This short anecdote suggests that *rituals* exist in technological practices such as cybersecurity, even if most cybersecurity rituals are not as clearly defined as prayer and have little explicit religious content. It also serves as a reminder of the cultural specificity of the Internet's origins, in contrast to its now global reach. Cyberspace is no longer the province only of those who pray towards Mecca satirically, and cybersecurity is a concern across nations, religions and cultures.

This article applies the concept of ritual to the cybersecurity "skills gap": the perceived lack of suitably qualified professionals necessary to tackle contemporary cybersecurity challenges. It draws on theories of expertise in International Relations (IR) to interpret this skills gap not as an objective absence of people or knowledge, but as an ideal socially constructed in tandem with an ever-widening sphere of cybersecurity threats. It proposes that cybersecurity expertise is best understood as *enacted*: as a skilled performance which satisfies decision-makers' demands for risk management. This alternative understanding of cybersecurity expertise as performance enables investigation of the types of

performance at key events which congregate experts together: cybersecurity conferences.

This article makes two key claims, which are empirically based on participant observation of cybersecurity conferences in the Middle East. First, that cybersecurity conferences are ritualized activities which create an expert community across international boundaries despite significant political and social differences. Second, that the ritualized physical separation between disinterested knowledge-sharing and commercial advertisement at these conferences enacts an ideal of "pure" cybersecurity expertise without which claims to knowledge would be greatly undermined.

This article has three main parts. The first introduces the cybersecurity skills gap and offers an alternative interpretation of cybersecurity expertise as performance. The second identifies conferences as a key site for participant observation and details the growth of cybersecurity conferences in the Middle East. The third applies the concept of ritual to these conferences. Following the conclusion, a postscript reflexively considers my role as a participant observer.

2. Cybersecurity Expertise

Cybersecurity experts are in great demand. A survey in 2015 predicted a "shortfall" of 1.5 million "information security professionals" by 2020 ((ISC)^2, 2015), and a year later another survey increased this forecast to a 2 million "shortage" of "cybersecurity professionals" by 2019 (ISACA, 2016). The message of these surveys, which are partly intended to raise awareness and business for those conducting them, is clear: there is a cybersecurity "skills gap", where "cyberattacks are growing, but the talent pool of defenders is not keeping pace" (ISACA, 2016). Current policy responses to this skills gap focus on adapting curricula, creating competitions to demonstrate technical skill, and training staff on-the-job (Vogel, 2016).

These policies are hampered by the unclear content of cybersecurity expertise. Cybersecurity professionals appear to require a vast range of skills from communications, compliance, data analytics and organizational psychology, as well as information technology (IT) (Pironti, 2013). This has led some to conclude that there is "surprisingly little consensus" around the cybersecurity skillset (Wolff, 2016). To counter this issue, the UK government has created a "cybersecurity body of knowledge" or CyBOK programme, which aims to build up a repository of core data for cybersecurity (Ensor, 2017). Like many observers of the lack of clarity in cybersecurity expertise, the creator of this programme attributes the problem solely to the "relative youth" of cybersecurity (Ensor, 2017). This suggests that cybersecurity is merely a "nascent epistemic community" (Stevens, 2012), which has yet to settle on its area of exclusive competence.

However, this narrative of novelty is deceptively simple. Novelty is not an external condition to which cybersecurity experts must respond, but rather a concept of time integral to the field itself. In other words, "the field of cyber security seems pervaded by a profound sense of frustration and disorientation at being trapped in an accelerating present, cut off by history" (Stevens, 2015, p. 93). Attributing the cybersecurity skills gap simply to an increasing rate of technological change—a permanent state of novelty—prevents analysis of the social and political ingredients which constitute cybersecurity as an expert domain.

Instead, contest is at the heart of cybersecurity expertise, which has been repeatedly refigured according to its political context (Barnard-Wills & Ashenden, 2012; Bendrath, 2001; Dunn Cavelty, 2008). Although an influential analysis of the social construction of cybersecurity argues that "cyber security can be seen as 'computer security' plus 'securitization'" (Hansen & Nissenbaum, 2009, p. 13), the suggestion that contest is limited to securitization—the framing of political issues as a security concern—implies that computer security itself is clearly defined. In contrast, others argue that the content of computer security, and how and where it overlaps with or adopts labels of cybersecurity and information security, are themselves key areas of contest (Shires & Smeets, 2017, p. 10).

To understand this contest, I draw on more sophisticated understandings of expertise which have emerged in IR (for overviews see Bueger, 2014; Cross, 2013). Such theories hold that, rather than simply importing expert knowledge from their academic or professional discipline into problems of societal and political importance, experts instead conduct what Seabrooke terms "epistemic arbitrage". This is where experts "mediate between knowledge pools for strategic advantage and, if successful, they can become the 'arbiters' on what knowledge and practices are most influential" (Seabrooke, 2014, p. 1). In cybersecurity, the proliferation of related disciplines allows experts to emphasise some areas over others in their interpretation of what counts as cybersecurity expertise, to "create new markets for their services and to challenge established orders" (Seabrooke, 2014, p. 13). This competitive rug-pulling in turn stretches and reshapes the domain itself, redistributing its increasing social, political and financial capital between software engineers and hardware manufacturers, lawyers, accountants and insurers, psychologists, intelligence professionals and political scientists.

These views of expertise focus not on expert knowledge in a static, codified form, but on expert *practice* and *performance*. In the words of legal scholar David Kennedy:

> Expert knowledge is human knowledge: a blend of conscious, semiconscious and wholly unconscious ideas, full of tensions and contradictions, inhabited by people who have projects and who think, speak and act strategically. Style and role count as much as content. (Kennedy, 2016, p. 278)

Kennedy here combines Seabrooke's view of experts as involved in power struggles, jostling for position and concerned with their individual projects, with an emphasis on how expertise is enacted or performed. To be an expert, one must *act* as an expert. For cybersecurity, this performance does not only include familiarity with Internet networks and computer programs, and the use of specialist tools. Most importantly, it includes the judgement and communication of certain risks, including reputational risk, threats to life and safety, financial risk, and national security. This expert performance has been described by some scholars as that of a "cyber-guru" (Quigley, Burns, & Stallard, 2015), who simplifies and overstates risks to maximise cybersecurity "hype" (Lee & Rid, 2014). Kennedy's view of expertise suggests in contrast that expert performance is essentially flexible, and that a nuanced and complex expression of risk can be more effective than exaggeration. In his words, "the uncertainty and ambivalence of professional knowledge may be the subtle secret of its success" (Kennedy, 2016, p. 10).

Cybersecurity experts learn this performance in several ways. One is to obtain cybersecurity qualifications, many of which claim to be "practical" and "hands-on", explicitly recognising the practice-based nature of expertise. Surveys indicate the popularity of this route; three quarters of respondents to one industry survey claimed that professional certifications are an effective way to demonstrate cybersecurity skills (Intel Security, 2016, p. 13). However, such qualifications suffer from contest over the power to become an 'arbiter' of professional practice, in Seabrooke's terms. As Wolff suggests, the "desire to profit from providing [cybersecurity] training may lead to too much competition" (Wolff, 2016), with the result that cybersecurity qualifications are of uncertain value. Supporting this view, other surveys indicate that experience is valued above all else: one found that experience was valued more highly than qualifications (UK HMGovernment, 2014, p. 15), and another reported that 93% of respondents thought experience was more important than qualifications (Sundaram, 2017). While all theories of expertise would agree that experience is important, the performance approach gives it an extra dimension. In this view, cybersecurity experience is not just a chance to collect further knowledge, but an apprenticeship in which professionals first mimic and then successfully inhabit the role of expert, pronouncing authoritatively on cybersecurity risks.

We can now reframe the concerns over a cybersecurity "skills gap" with which I began this section. The skills gap stems from a supposed mismatch between the level of risk and the number of cybersecurity experts. However, we can now see that this level of risk is itself the result of a successful performance by those experts. Crucially, cybersecurity risk expands as more knowledge pools are brought to bear on cybersecurity, with ever more additions to the "attack surface" and potential means for illegitimate access. As long as cybersecurity continues to accrue social and political capital, this proliferation of relevant domains will continue, and the required repertoire of the "sufficiently skilled" cybersecurity professional will continue to expand. A gap is the wrong metaphor for this process, as it obscures the connection between expanding expert performance and increasing risk. Instead of focusing on how to 'close the gap', I examine the performances themselves.

3. Cybersecurity Conferences

Cybersecurity expertise is performed in many places, not least in the day-to-day work of cybersecurity professionals. One way of accessing this performance is through participant observation. Participant observation, defined as "immersion in a community, a cohort, a locale, or a cluster of related subject positions" (Schatz, 2009), is closely associated with a commitment to ethnographic modes of research, which "chronicle aspects of lived experience and…place that experience in conversation with prevailing scholarly themes" (Wedeen, 2010). Some scholars have attempted to access a professional cybersecurity environment—security operations centres, or SOCs—using participant observation. These scholars have identified several new aspects of cybersecurity expert performance, including detailed information about workflows and reflections on their perceived status, described as follows:

> SOCs face a constant challenge in in justifying their value to the management. Security monitoring, unlike in any other business, cannot be quantified through profit margins. Nobody notices the value of a SOC as long as there is no major breach. (Sundaramurthy, Case, Truong, Zomlot, & Hoffmann, 2014, p. 49)

This quotation anticipates an underlying tension between financial incentives and cybersecurity expertise to which I will return in the last section. In this section I detail the empirical site of participant observation on which my argument is based. SOCs and other daily professional environments are not the only locations of expert performance, which also occurs at professional conferences. As Howard describes in his study of digital democracy activists, conferences, although "occurring in sterile hotels…still represent key events full of important social interaction" (Howard, 2002, p. 561). Despite this potential, conferences are not a traditional ethnographic site, as they are short, happen infrequently, and move between different geographical locations. This has posed a methodological problem for anthropologists, who have conceptualised conferences and similar phenomena in several ways: as "transitory" sites; as together forming a "multi-site" ethnography, or as forming one geographically discontinuous site (Falzon, 2009, p. 17).

One region where cybersecurity conferences have become a regular occurrence is in the Middle East. Using structured Internet searches, with search terms based

on cybersecurity and cognate terms such as digital or information security, with "Middle East" as an initial guiding qualifier, I identified 165 conferences within these parameters between 2007 and 2016. Larger technology or security conferences that included cybersecurity as a minor topic were excluded. The rise in the frequency of these conferences was significant, from 2 in 2007 to 28 in 2016, as shown in Figure 1. The conferences included some hosted by cybersecurity vendors, others organised by professional events companies, and some with support from governments or international organisations. The average attendance based on media reports was around 200 people, excluding one large outlier (GISEC, with around 4,000 attendees). In numerical terms, this trend is not especially surprising. The increase in Middle East cybersecurity conferences could probably be replicated in many areas of the world, as during that decade cybersecurity grew significantly in the global consciousness. However, the geographical grouping of these conferences is not intuitively obvious, in two ways.

First, although these conferences are often labelled expansively, as "Middle East", "Middle East and North Africa" (MENA), or as "Arab Region", these conferences nearly all take place in Egypt and the states of the Gulf Cooperation Council (GCC): Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates (UAE).[1] This narrower representation within the wider Middle East stems from several political factors. Other countries in the region are the site of severe conflicts, and although the Gulf states above are intimately involved in these conflicts their domestic environments have been relatively unaffected. This stability is connected to commercial incentives for holding the conferences: the GCC states are the richest in the Middle East due to extensive natural resources, and have—to various extents—developed their domestic infrastructure to attract global capital (Held & Ulrichsen, 2011). Cybersecurity concerns in these states are much more similar to the concerns of other wealthy, highly connected states than their immediate neighbours (in comparison, Yemen, the only non-GCC Arab state in the Gulf, has very different Internet issues (Dalek, Deibert, McKune, Gill, & Senft, 2015).

Two other key countries in the Middle East cybersecurity landscape, Iran and Israel, are not represented in the conferences above, for different reasons. Iran is seen by many as a geopolitical rival to Saudi Arabia and has conflicted relationships with other Gulf states. Furthermore, Iran is perceived as a threat to the US, which has a longstanding presence in Egypt and the Gulf, due to its nuclear ambitions, regional influence, and reciprocal hostile cyber activity. Israel, in contrast, is a global cybersecurity hub in its own right, with a strong military-based cybersecurity sector (Behar, 2016) and traditional isolation from the Arab world, although covert cooperation exists in various cybersecurity-related areas (Caspit, 2016; Donaghy, 2015; Marczak & Scott-Railton, 2016). In sum, the narrowed definition of Middle East cybersecurity therefore stems not only from domestic characteristics and commercial incentives, but also wider international relations in the region.

However, this grouping of conferences is also surprisingly inclusive, as Egypt and the GCC states have substantial differences which affect their cybersecurity posture. Egypt does not have the same financial advantages due to a large population and relative lack of natural resources, although it also has an outsized military and security sector and commensurate budgets. The Arab Spring was experienced very differently, with Egypt un-

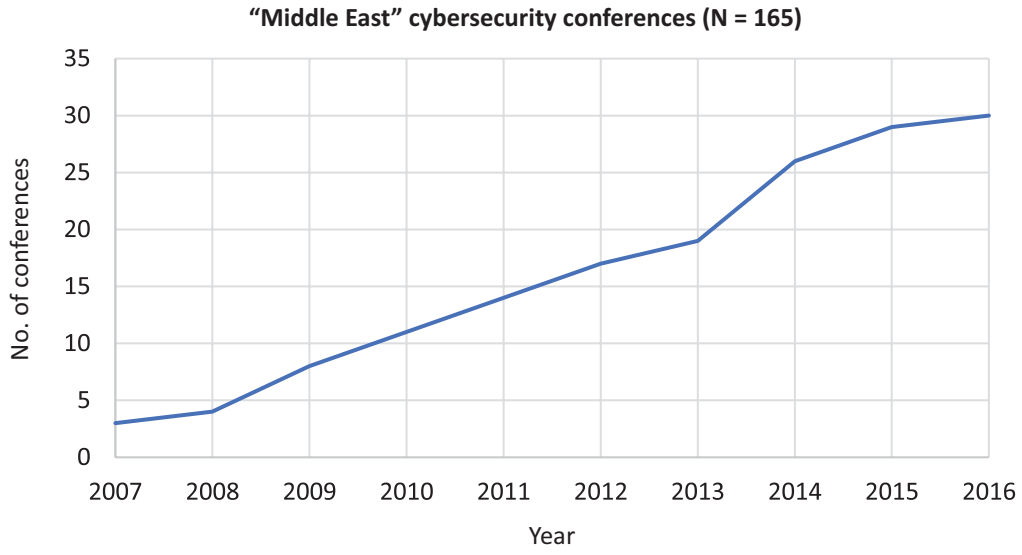

Figure 1. "Middle East" cybersecurity conferences.

[1] The exception was the MENA Information Security conference 2011 in Amman, Jordan. For further discussion about the scope of this term, see Bonine, Amanat and Gasper (2011).

dergoing repeated changes of government and the GCC cooperating in repression against activists (Matthiesen, 2013). While Egypt has broader issues with Internet adoption, and has taken more drastic Internet policies than the GCC—the Egyptian government resorted to a complete severance of Internet connections following the January 2011 revolution—the GCC states have incorporated restrictions on the public sphere in keeping with a cautious approach to new communications technologies due to their potential political effects (Shires, in press). Finally, there are significant political rifts within the GCC, exacerbated since the Qatar crisis in June 2017, leading to a "quartet" of Egypt, Bahrain, Saudi Arabia and the UAE separating from the other three states.

Given these diverse regional factors, the spread of conferences across Egypt and the GCC states is not intuitive and creates a "site" for ethnographic observation in cybersecurity stretching across and between other socio-political divides. I conducted participant observation at seven cybersecurity conferences in the region, summarised in Table 1. These conferences were chosen due to the length of time held, the range of organizing bodies and topic, and more prosaic research characteristics such as budget and time constraints. At these conferences, I repeatedly met the same community of conference speakers, and the same companies and government organizations, which suggests that these conferences constitute a unique regional space in which to perform cybersecurity expertise.

This personal observation of a distinctive cybersecurity community is supported by a wider analysis of conference speakers. I created a dataset of all invited speakers at the 165 cybersecurity conferences in the region, based on a range of open sources including conference programmes and surrounding media. This dataset identified which conference series were attended by each speaker and the number of conferences within each series attended by that speaker. Of the total number of speakers (1,177), only 96 (8%) had spoken at more than three conferences *and* across more than one conference series (and these had often spoken at many more). This indicates that although many individuals participate as speakers at these cybersecurity conferences, a relatively small number do so consistently over time and are recognised as cybersecurity experts by several conference organisers.[2] In the next section, I use the concept of ritual to explore the conference performances of this expert community in more detail.

4. Ritualized Conferences

Cybersecurity conferences are highly ritualized activities. Ritual was originally a term for the script used to instruct religious practices or rites, but has become commonly used to refer to religious practices themselves (Stewart & Strathern, 2014). However, many anthropologists argue that a fundamental distinction between religious and secular is unhelpful in the analysis of rituals (Grimes,

Table 1. Middle East cybersecurity conferences attended.

Name	Location	Date attended	Years held (to date)	Organizing body
ITU Arab Region Cybersecurity Summit	Sharm El Sheikh	October 2016	2014–2017	Egypt National Telecommunications Regulatory Authority (NTRA), International Telecommunications Union (ITU)
FIRST Middle East	Sharm El Sheikh	November 2016	2016	Egyptian NTRA, FIRST (non-profit association of CERTs)
Cairo Security Camp	Cairo	November 2016	2010–2017	Bluekaizen (cybersecurity company)
RSA MENA	Abu Dhabi	November 2016	2012–2017 (others in Qatar and Saudi Arabia)	RSA (cybersecurity and events company)
Cybersecurity for Critical Assets MENA	Dubai	November 2016	2015–2016	Qatalyst Global (cybersecurity events company)
Middle East Cybersecurity	Riyadh	April 2017	2015–2017	Nispana (events company)
ITU Arab Region Cybersecurity Summit	Muscat	November 2017	As above	Oman Information Technology Authority (ITA), ITU

[2] A further step in this analysis would compare this attendance to other regions or other countries in the region such as Iran or Israel. Although space constraints prevent such an analysis here, conversations with the "super-speakers" identified above suggest that they rarely if ever participate in conferences in those two countries.

2006). Instead, we can see all activities as lying on a scale of ritualization with several dimensions, including formalism, disciplined invariance, rule-governance, and symbolism (Bell, 2009, p. 138). Highly ritualized activities possess these characteristics in greater intensity or quantity than the surrounding environment, and these characteristics are often found together, in a mutually reinforcing manner.

The ritualization of cybersecurity conferences is facilitated by their physical and temporal organization, which follows a standard pattern for business conferences. The cybersecurity conferences I attended all had a central presentation room for "keynote" speakers, as well as several breakout rooms for smaller-scale discussions, with scheduling governed by several written and unwritten rules: printed schedules, food and drink requirements, unexpected absences, and the importance of the speaker. There was a separate area for marketing stands by cybersecurity companies, who paid for spaces. Some companies paid for higher levels of sponsorship, in return for a keynote slot and branding on presentations, notes, and conference paraphernalia such as lanyards, which serve as constant symbolic reminders of their contribution. This overall format is largely due to what Bell terms 'disciplined invariance'—i.e., deliberate repetition—created by the logistical and financial assemblage behind the conference. Although the conferences themselves were often hosted by a national government organization involved in cybersecurity, the organization of the conference was outsourced to events companies who imprint standard formats onto the cybersecurity community (following Rappaport's formulation of the conditions of ritual, conferences are largely "encoded by other than performers"; Rappaport, 1999, p. 32). As such, these conferences are ritualized in the sense that they are more rule-governed, invariant, and formalised than the day-to-day work of cybersecurity professionals.

To understand how this ritualization enhances the performance of cybersecurity expertise, we can compare cybersecurity conferences to similar cases. In a closely related context, the concept of ritual has been used to argue that "hacker" conferences embody a particular "lifeworld", which is brought into being through hackers spending short, intense periods of time together focusing on their common passion (Coleman, 2010). However, in her participant observation Coleman also detected differences in the "moral economy" of conferences:

> The differences between the American Psychiatric Association annual meetings, where doctors are dressed in suits and mill about during the day at San Francisco's Moscone Center, retiring individually in the evening to a luxury San Francisco high-rise hotel after a nice dinner, and the outdoor festival held by European hackers, where bodies are clothed in tee-shirts and shorts (if that), and many participants can be found sleeping together under the stars of the night, are difficult to deny. (Coleman, 2010, p. 67)

Despite their similar content to the hacker conferences described by Coleman—malware analysis, details of vulnerabilities, stories of famous hacks, and so on—cybersecurity conferences appear to have as much in common with the drab medical gatherings to which she juxtaposes the hackers' "ritual celebration". The cybersecurity conferences I attended were held in luxury hotels, with high-quality food and drink available throughout. Formal dress was required (Figure 2). As is the case for cybersecurity and technology sectors more generally, there were far more men than women at these

Figure 2. Arab Region Cybersecurity Summit 2017 (Source: Author's own photo).

conferences, and only 4 of the 96 frequent speakers (4%) identified in Part 3 were women.[3] Although the post-conference recreational activities occasionally resembled hacker conferences more closely—for example, poetry recitation on a trip to the beach—there was just as much "milling about". If cybersecurity conferences create a lifeworld, it is not that of the hacker.

Given these differences, another comparison may be useful. Scholars have also conducted participant observation at trade fairs for security products (defence technologies, policing equipment, surveillance, and so on). These fairs have a shared genealogy with the cybersecurity conferences I attended, in that some cybersecurity conferences in the Middle East are offshoots of larger defence and security fairs, and defence companies are central figures in the cybersecurity market. In an analysis of a long-running trade fair in the UK, Alexander argues that "these spaces are pivotal in the dissemination, propagation, and reformulation of changing attitudes towards security" (Alexander, 2014, p. 18), as they underpin the "logic of a particular mind-set regarding what it means to consume security as a commodity" (Alexander, 2014).

Although cybersecurity conferences also involve the sharing of a security mind-set, Alexander's description of security fairs as hotspots for the "intensive exchange of knowledge [and] new ideas" only partly resonates with my participant observation. Although cybersecurity conference programs are full of talks on professional topics, most delegates spend little time listening to them. Other than the keynote speeches, which are well attended partly due to greater interest and partly greater enforcement from the conference organizers, there is ample opportunity to spend time at trade stalls, refreshment places, in hotel lobbies or (if the heat permits) outside at lengthy cigarette breaks. Panel discussions often elicit few questions and little audience participation. When delegates are in the audience, most of their time is spent on devices; sometimes working, but also as an instinctive response to what is almost downtime. Networking is a large part of these conferences, but they also offer a space to relax, to catch up on work, and to spend time away from the desk.

Given the unclear attention paid by conference attendees to formal methods of disseminating knowledge, I use ritual theorists' focus on space (e.g. Turner, 1977), to show how the shared format of these conferences shapes the performance of expertise. The fundamental division in this physical space is between the outer layer of company-branded booths and the inner layer of presentation rooms; in other words, between a space for commerce (the trade stands) and a space for knowledge (the central auditorium and breakout rooms). Speakers conform to this ritual division in their on-stage performance, disclaiming any "sales pitch" when delivering talks, even about their product, although this is often undermined by the company copyright of their slides. The conference space is therefore an explicit acknowledgement and simultaneous separation of both the myriad commercial incentives for conference organizers, hosts, speakers, and attendees at the outer layer, *and* their claims to possess an independent and unbiased expert knowledge at the inner layer.

The separation of knowledge and commerce shapes cybersecurity expertise in two ways, enhanced by the formalism and invariance identified above. First, this separation expresses an ideal version of cybersecurity expertise. Despite the competitive political and commercial struggles between individuals and organizations that exist in any expert domain, this separation creates a guiding principle or myth of "pure" cybersecurity knowledge, untainted by these struggles, which encourages the formation of the discipline itself as a new area of disinterested inquiry. Second, this physical separation inscribes the ability to alter their performance between these spaces—to shift repertoire—as a core skill for cybersecurity experts. The same people deliver their independent expert judgement on stage, and then an unashamedly partisan view of their superior product after returning to their booth. I do not mean to imply that either is incorrect, or that to do both is necessarily hypocritical, but that this duality is imposed by the separation of the conference space itself. Cybersecurity expertise is thus not just the successful performance of risk management, but one which is essentially flexible, with several registers and the capacity for context-based improvisation.

This physical separation and performative disconnect between knowledge and commerce suggests that cybersecurity expertise does not match either close comparison above: it is neither an explicit commodification of security nor a liberated hacker's lifeworld. Instead, the heart of cybersecurity expertise is the simultaneous embrace of an underlying commercial logic *and* the ideal of a neutral judgement of new technological risks. This double movement exists elsewhere in cybersecurity: in the contest over cybersecurity qualifications, in the challenges of cybersecurity public-private partnerships (Carr, 2016), and the rise of the "cyber-industrial complex" (Deibert & Rohozinski, 2011). However, conferences, as ritualized occasions for the performance of expertise *to other experts*, uniquely equip cybersecurity professionals with the repertoire incorporating this double movement, and so are key sites for the production of cybersecurity expertise more broadly.

5. Conclusion

This article has completed three tasks. First, it reoriented discussions around cybersecurity expertise, often

[3] This may be changing: conversations at these conferences suggest that around half of citizens training in cybersecurity in the smaller Gulf states are female (themselves a small proportion of cybersecurity professionals overall, due to the overwhelmingly male expatriate technology community). These simple gender proportions do not accurately portray the complexities of gender performance (both masculinities and femininities) in cybersecurity in the region, which deserve a separate study.

expressed as a skills gap, towards a conception of expertise as successful performance. Cybersecurity expertise should not be thought of as a gap to be closed, because the requirements for successful performance grow together with the widening of the domain. Second, it identified cybersecurity conferences as key sites of expert performance and used the example of cybersecurity conferences in the Middle East to show how such conferences bring together a diverse community across international divisions. Third, it analysed these conferences as ritualized activities, which physically separate commercial transactions and knowledge production in a way which makes possible the emergence of cybersecurity expertise itself as a body of knowledge.

The main limitation of this article is that, due to space constraints, it has focused only on the spatial performance of expertise in the overall conference environment. Further work would distinguish more finely between the different genealogies of cybersecurity professionals (defence, intelligence, IT, engineering, and so on), and would track the effect of this professional "habitus" on cybersecurity worldviews, analysing not just commercial underpinnings but also wider threat construction. A related limitation is that this article relies on personal observation of expert performance (albeit informed by extensive interaction with the expert community) but does not investigate the perception of this performance by experts themselves, or otherwise provide a space for their voices. Further work, drawing explicitly on interviews and conference discourse, would correct this imbalance and provide a more comprehensive picture of cybersecurity expert performance.

This investigation has several implications for other areas of IR. First, it provides a performance-based interpretation of the dynamics of a growing arena of knowledge which could be applied to other skilled domains in international politics. Second, it provides an empirical treatment of cybersecurity conferences in the Middle East, which crosses familiar boundaries and offers a new reading of regional dynamics with implications outside cybersecurity. Finally, it underlines the importance of ritual in analysing the dynamics of international behaviour, especially conferences and conference-like events, which are frequent occurrences in international politics on topics ranging from peace negotiations to climate change treaties. Some of the ritualized characteristics noted here may appear, with similar symbolism, in these other areas.

Postscript

In this postscript, I briefly reflect on my participation in the cybersecurity conferences above. Reflexive analysis of my own epistemological, moral, and other commitments is a key aspect of participant observation. This is especially important as I use the concept of ritual, which imputes significance to an activity which may not be expressed or recognised by other participants. In this analysis, I attempted to avoid two related pitfalls. The first is an assumption of superiority: that the interpretation offered here is somehow truer, better, or more accurate than an "inside" interpretation. The second is a refusal of symmetry. As Latour notes, ritual and its associated concepts are often reserved for those who are assumed not to be "Modern" and are not applied symmetrically to Modern practices (Latour, 2010).

To counter these pitfalls, the analysis above is an intervention in a conversation not only with other academics, but with conference participants as well, to be judged and critiqued on both levels. Furthermore, cybersecurity professionals, as highly qualified graduates of advanced engineering and scientific courses, are as Modern in Latour's sense, if not more so, than any social scientist who works with and alongside them. Consequently, my methods and conclusion are as open to critique by them as much as their epistemological stance is questioned by this article.

Although the empirical site is the Middle East, rather than the "West", I do not mean to imply homogeneity. This community includes people from across the world, with varied religious, political, and social backgrounds. Countries of origin for speakers include South Korea, Singapore, China, Europe and the US, and conference attendees with a more permanent presence in the region include expatriate workers from South Asia and Europe, as well as immigrants within the region itself (notably Egyptian nationals throughout the GCC, due to proximity and attractive market conditions). While some religious and cultural formulations are nearly always present (such as religious introductions to formal speech used instinctively by many Muslims and sometimes attempted sympathetically by non-Muslim presenters), there are as many moments which present a different set of cultural and linguistic associations and hierarchies, such as native Arabic speakers who find it easier to switch into English to present on technical cybersecurity topics.

Nonetheless, my own profile as a white male and a native English speaker with working Arabic proficiency was important. I was quickly put into specific categories—consultant, guest speaker—by my interlocutors, and treated in a way which would have changed had my gender, ethnicity, or language been different. I wore a badge accurately describing me as a member of the University of Oxford, which also had a significant impact on my reception. As a recognisable label with extensive social and academic associations, "Oxford" both increased my acceptance and made it suspicious: as one interlocutor mentioned, pointing out Oxford University's connection to the UK intelligence community, "they don't know who you are, you come from a country with a bad history in these things, they don't know what you will do with the information".

Acknowledgments

I thank the UK Economic Social Research Council and the University of Oxford for funding this research, and the

members of the Cyber Studies Programme and Centre for Technology and Global Affairs at the University of Oxford for their stimulating conversations on the issues in this article.

Conflict of Interests

The author declares no conflict of interests.

References

(ISC)^2. (2015, April 17). *Workforce shortfall due to hiring difficulties despite rising salaries, increased budgets and high job satisfaction rate. (ISC)^2*. Retrieved from http://blog.isc2.org/isc2_blog/2015/04/isc-study-workforce-shortfall-due-to-hiring-difficulties-despite-rising-salaries-increased-budgets-a.html

Alexander, J. (2014). *Promoting security imaginaries: An analysis of the market for everyday security solutions* (Doctoral dissertation). University of Manchester. Manchester, UK.

Barnard-Wills, D., & Ashenden, D. (2012). Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture*, *15*(2), 110–123.

Behar, R. (2016, May 11). Inside Israel's secret startup machine. *Forbes*. Retrieved from https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/#6c3400ca1a51

Bell, C. (2009). *Ritual: Perspectives and dimensions, revised edition*. New York, NY: Oxford University Press.

Bendrath, R. (2001). The cyberwar debate: Perception and politics in US critical infrastructure protection. *Information & Security*, *7*, 80–103.

Bonine, M. E., Amanat, A., & Gasper, M. E. (Eds.). (2011). *Is there a Middle East? The evolution of a geopolitical concept*. Stanford, CA: Stanford University Press.

Bueger, C. (2014). From expert communities to epistemic arrangements: Situating expertise in International Relations. In M. Mayer, M. Carpes, & R. Knoblich (Eds.), *The global politics of science and technology* (Vol. 1, pp. 39–54). Heidelberg: Springer Verlag GmbH.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62.

Caspit, B. (2016, February 29). The Israeli–Egyptian love affair. *The Washington PAC*. Retrieved from http://www.washingtonpac.com/Articles%20of%20Interest/israeli_egyptian_love_affair.htm

Coleman, G. (2010). The hacker conference: A ritual condensation and celebration of a lifeworld. *Anthropological Quarterly*, *83*(1), 47–72.

Cross, M. K. D. (2013). Rethinking epistemic communities twenty years later. *Review of International Studies*, *39*(1), 137–160.

Dalek, J., Deibert, R. J., McKune, S., Gill, P., & Senft, A. (2015, October 21). Information controls during military operations: The case of Yemen. *Citizen Lab*. Retrieved from https://citizenlab.ca/2015/10/information-controls-military-operations-yemen

Deibert, R. J., & Rohozinski, R. (2011, March 28). The new cyber military-industrial complex. *The Globe and Mail*. Retrieved from https://www.theglobeandmail.com/opinion/the-new-cyber-military-industrial-complex/article573990

Donaghy, R. (2015, February 28). Falcon eye: The Israeli-installed mass civil surveillance system of Abu Dhabi. *Middle East Eye*. Retrieved from http://www.middleeasteye.net/news/uae-israel-surveillance-2104952769

Dunn Cavelty, M. (2008). *Cyber-security and threat politics*. London and New York, NY: Routledge.

Ensor, C. (2017, July 26). Building the cyber security body of knowledge. *National Cyber Security Centre*. Retrieved from https://www.ncsc.gov.uk/blog-post/building-cyber-security-body-knowledge-0

Falzon, M.-A. (Ed.). (2009). *Multi-sited ethnography: Theory, praxis and locality in contemporary research*. Farnham and Burlington, VT: Routledge.

Grimes, R. L. (2006). *Rite out of place: Ritual, media, and the arts*. Oxford and New York, NY: Oxford University Press.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175.

Held, D., & Ulrichsen, K. (Eds.). (2011). *The transformation of the Gulf: Politics, economics and the global order*. Abingdon, Oxon, and New York, NY: Routledge.

Howard, P. N. (2002). Network ethnography and the hypermedia organization: New media, new organizations, new methods. *New Media & Society*, *4*(4), 550–574.

Intel Security. (2016). *Hacking the skills shortage: A study of the international shortage in cybersecurity skills*. Washington, DC: Centre for Strategic and International Studies.

Isaacson, W. (2015). *Innovators: How a group of inventors, hackers, geniuses and geeks created the digital revolution*. New York, NY: Simon & Schuster.

ISACA. (2016, January). *2016 cybersecurity skills gap. Cybersecurity nexus*. Retrieved from https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg

Kennedy, D. (2016). *A world of struggle: How power, law, and expertise shape global political economy*. Princeton, NJ: Princeton University Press.

Latour, B. (2010). *On the modern cult of the factish gods*. Durham NC, and London: Duke University Press Books.

Lee, R. M., & Rid, T. (2014). OMG cyber! *The RUSI Journal*, *159*(5), 4–12.

Marczak, B., & Scott-Railton, J. (2016, August 24). The million dollar dissident: NSO group's iPhone Zero-days used against a UAE human rights defender. *Citizen Lab*. Retrieved from https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae

Matthiesen, T. (2013). *Sectarian Gulf: Bahrain, Saudi Arabia and the Arab Spring that wasn't*. Stanford, CA: Stanford University Press.

Pironti, J. (2013, January 15). The changing role of security professionals. *Info Security*. Retrieved from https://www.infosecurity-magazine.com/magazine-features/the-changing-role-of-security-professionals

Quigley, K., Burns, C., & Stallard, K. (2015). 'Cyber gurus'. *Government Information Quarterly*, *32*(2), 108–117.

Rappaport, R. A. (1999). *Ritual and religion in the making of humanity*. Cambridge: Cambridge University Press.

Schatz, E. (Ed.). (2009). *Political ethnography: What immersion contributes to the study of power*. Chicago, IL, and London: University of Chicago Press.

Seabrooke, L. (2014). Epistemic arbitrage: Transnational professional knowledge in action. *Journal of Professions and Organization*, *1*(1), 49–64.

Shires, J. (in press). Cybersecurity governance in the GCC. In R. Ellis & V. Mohan (Eds.), *Rewired: Cybersecurity governance*. Hoboken, NJ: Wiley-Blackwell.

Shires, J., & Smeets, M. (2017, December). *Contesting 'cyber'*. Washington, DC: New America Foundation.

Stevens, T. (2012, March 27). Norms, epistemic communities and the global cyber security assemblage. *E-International Relations*. Retrieved from http://www.e-ir.info/2012/03/27/norms-epistemic-communities-and-the-global-cyber-security-assemblage

Stevens, T. (2015). *Cyber security and the politics of time*. Cambridge: Cambridge University Press.

Stewart, P. J., & Strathern, A. (2014). *Ritual: Key concepts in religion*. London and New York, NY: Bloomsbury Academic.

Sundaram, A. (2017, March 20). Security certifications are useless, right? *Info Security*. Retrieved from https://www.infosecurity-magazine.com/news-features/security-certifications-useless

Sundaramurthy, S. C., Case, J., Truong, T., Zomlot, L., & Hoffmann, M. (2014). A tale of three security operation centers. In R. Biddle & B. Chu (Eds.), *Proceedings of the 2014 ACM workshop on security information workers* (pp. 43–50). New York, NY: ACM.

Turner, V. (1977). Variations on a theme of liminality. In S. F. Moore & B. G. Myerhoff (Eds.), *Secular ritual* (pp. 36–52). Assen: Van Gorcum.

UK HMGovernment. (2014). *Cyber security skills: Business perspectives and government's next steps*. London: Department for Business Innovation and Skills.

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, *4*(2), 32–46.

Wedeen, L. (2010). Reflections on ethnographic work in political science. *Annual Review of Political Science*, *13*(1), 255–272.

Wolff, J. (2016, April 14). Why computer science programs don't require cybersecurity classes. *Slate*. Retrieved from http://www.slate.com/articles/technology/future_tense/2016/04/why_computer_science_programs_don_t_require_cybersecurity_classes.html

About the Author

James Shires is a DPhil candidate in International Relations and a Research Affiliate at the Centre for Technology and Global Affairs, at the Department of Politics and International Relations, University of Oxford. He has an MSc in Global Governance and Public Policy from Birkbeck College, University of London, a BA in Philosophy from the University of Cambridge.